

An Algebraic View to Gradient Descent Decoding

M. Borges Quintana and M.A. Borges Trenard

Facultad de Matemática y Computación

Universidad de Oriente

Santiago de Cuba, Cuba

mijail@mbq.uo.edu.cu mborges@mabt.uo.edu.cu

I. Márquez-Corbella and E. Martínez-Moro

SINGACOM group

Universidad de Valladolid

Castilla, Spain

http://www.singacom.uva.es
imarquez@agt.uva.es edgar@maf.uva.es

Abstract—There are two gradient descent decoding procedures for binary codes proposed independently by Liebler and by Ashikhmin and Barg. Liebler in his paper [15] mentions that both algorithms have the same philosophy but in fact they are rather different. The purpose of this communication is to show that both algorithms can be seen as two ways of understanding the reduction process algebraic monoid structure related to the code. The main tool used for showing this is the Gröbner representation of the monoid associated to the linear code.

I. INTRODUCTION

From now on a code \mathcal{C} will be a binary linear code of length n and dimension k , i.e. a k -dimensional linear subspace of \mathbb{F}_2^n where \mathbb{F}_2 is the field of two elements. Let $d(\cdot, \cdot)$, $\text{wt}(\cdot)$ be the Hamming distance and the Hamming weight on \mathbb{F}_2^n respectively. Let d denote the minimal Hamming distance of the code \mathcal{C} .

Given a code \mathcal{C} and let \mathbf{r} be a received word in \mathbb{F}_2^n the complete decoding problem (CDP) addresses to determine a codeword $\mathbf{c} \in \mathcal{C}$ that is closest to \mathbf{r} . The t -bounded distance decoding problem (t -BDP) is to determine a codeword $\mathbf{c} \in \mathcal{C}$ such that $d(\mathbf{r}, \mathbf{c}) \leq t$ if such codeword exists. If $t = \lfloor \frac{(d-1)}{2} \rfloor$ then the solution of the t -BDP is unique and if $t = \rho$ the covering radius then t -BDP is the same as CDP. Both problems are quite related to the coset weights problem (t -CWP) that can be stated as follows, given a binary $r \times n$ matrix and an r -dimensional vector \mathbf{s} and $t \in \mathbb{Z}_{\geq 0}$, does a binary vector $\mathbf{e} \in \mathbb{F}_2^n$ exist such that $w(\mathbf{e}) \leq t$ and $H\mathbf{e} = \mathbf{s}$? All these problems have been shown to be NP-complete [2], [3] even if preprocessing is allowed [10].

Recently complete decoding and particularly gradient descent complete decoding have gain new interest related to the decoding of LDPC codes, in fact Liebler in [15] says that there is not a clear answer to the question of which parameters of a code could help to recognize and to implement a gradient descent decoding function for the code having the coset leaders as output. Moreover in the same paper the author makes a distinction between two gradient descent decoding algorithms (GDDA) that we will denote by leader GDDA (l-GDDA) and test-set GDDA (ts-GDDA) that are claimed to be different (see section II for formal definitions of the algorithms).

The purpose of this work is to show that both algorithms can be seen as two ways of understanding the reduction process within algebraic monoid structure related to the code. For that

aim the main tool used will be the Gröbner representation of the monoid associated to the linear code [4]. The structure of the paper will be as follows. Section II will show the two gradient descent decoding algorithms, Section III will give a brief review to the Gröbner representation of a code and its associate structures. Section IV will show the main result, i.e. how the two GDD algorithms can be seen as reduction associated to the Gröbner representation of the code.

II. GRADIENT DESCENT DECODING ALGORITHMS

In this section we will briefly describe two gradient descent decoding algorithms. The first one will be the *leader GDDA* and can be stated as follows. Let us denote by $\bar{\mathbf{y}}$ the coset in $\mathbb{F}_2^n/\mathcal{C}$ containing \mathbf{y} and $\text{wt}(\bar{\mathbf{y}})$ the weight of one of its leaders.

Algorithm 1. l-GDDA

Input: \mathbf{r} the received word.

Output: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to \mathbf{r}

Repeat until $\text{wt}(\bar{\mathbf{r}}) = 0$

a) Compute \mathbf{r}' such that $\text{wt}(\mathbf{r} - \mathbf{r}') = 1$ and $\text{wt}(\bar{\mathbf{r}}) \geq \text{wt}(\bar{\mathbf{r}}')$

b) $\mathbf{r} \leftarrow \mathbf{r}'$

Return $\mathbf{c} = \mathbf{r}$.

Note that in each of the steps of the algorithm the vector \mathbf{r} changes between different cosets of $\mathbb{F}_2^n/\mathcal{C}$ until it arrives to the $\bar{\mathbf{0}}$ coset, i.e. the code itself. This is essentially the same as syndrome decoding broken up in smaller steps. The paper [15] presents the first such construction method of a gradient function $\gamma : \mathbb{F}_2^n/\mathcal{C} \rightarrow \mathbb{Z}$ such that is a strictly increasing function of $\text{wt}(\bar{\mathbf{m}})$ for performing such a l-GDDA.

For understanding the next GDD algorithm we will need some knowledge of minimal (support) codewords. The *support of a codeword* $\mathbf{c} \in \mathcal{C}$ will be the set of its non-zero positions, i.e. $\text{supp}(\mathbf{c}) = \{i \mid c_i \neq 0\}$.

Definition 2. A codeword \mathbf{m} in the code \mathcal{C} is said to be minimal if there is no other codeword $\mathbf{c} \in \mathcal{C}$ such that

$$\text{supp}(\mathbf{c}) \subseteq \text{supp}(\mathbf{m}).$$

We will denote by $\mathcal{M}_{\mathcal{C}}$ the set of all the minimal codewords of \mathcal{C} . The usual way of defining a steepest descent method in the Hamming space is to construct a *test set* $\mathcal{T} \subseteq \mathbb{F}_2^n$. A test set is a set of codewords such that every word \mathbf{y} either lies in $V(\mathbf{0})$ (the Voronoy region of the all-zero vector) or there is a

$\mathbf{t} \in \mathcal{T}$ such that $\text{wt}(\mathbf{y} - \mathbf{t}) < \text{wt}(\mathbf{y})$. The gradient-like or *test set GDDA* is stated as follows (see [2] for further details and correctness of the algorithm)

Algorithm 3. *ts-GDDA*

Input: \mathbf{r} the received word.

Output: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to \mathbf{r}
 $\mathbf{c} \leftarrow \mathbf{0}$

Repeat until no $\mathbf{t} \in \mathcal{T}$ is found such that

$$\text{wt}(\mathbf{r} - \mathbf{t}) < \text{wt}(\mathbf{r})$$

a) $\mathbf{c} \leftarrow \mathbf{c} + \mathbf{t}$

b) $\mathbf{r} \leftarrow \mathbf{r} - \mathbf{t}$

Return \mathbf{c} .

It is pointed in [2] that setting $\mathcal{T} = \mathcal{M}_{\mathcal{C}}$ in the previous Algorithm 3 the so call minimal vector algorithm performs complete minimum distance decoding.

III. GRÖBNER REPRESENTATION AND RELATED STRUCTURES

In this section we will show some basic results on the Gröbner representation of a code \mathcal{C} . In fact it is related to the additive representation of the monoid $\mathbb{F}_2^n/\mathcal{C}$. We will try to keep this section as Gröbner basis technology-free as possible. For some references on Gröbner representations of codes and its implementations see [4], [5], [6], [8], [7]. Let $\mathbf{e}_i \in \mathbb{F}_2^n$ be the vector with all its entries 0 but a 1 in the i th-position.

Definition 4. A *Gröbner representation* of $\mathbb{F}_2^n/\mathcal{C}$ is a pair N, ϕ where N is a transversal of the cosets in $\mathbb{F}_2^n/\mathcal{C}$ (i.e. one element of each coset) such that $\mathbf{0} \in N$ and for each $\mathbf{n} \in N \setminus \{\mathbf{0}\}$ there exists a \mathbf{e}_i , $i \in \{1, 2, \dots, n\}$ such that $\mathbf{n} = \mathbf{n}' + \mathbf{e}_i$ with $\mathbf{n}' \in N$ and a mapping

$$\phi : N \times \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\} \rightarrow N$$

such that the image of the pair $(\mathbf{n}, \mathbf{e}_i)$ is the element representing the coset that contains $\mathbf{n} + \mathbf{e}_i$.

The word Gröbner is not casual as we will see it with the following construction. Let us consider the binomial ideal

$$\mathcal{I}_{\mathcal{C}} = \langle \{\mathbf{x}^{\mathbf{a}^{\mathbf{w}_1}} - \mathbf{x}^{\mathbf{a}^{\mathbf{w}_2}} \mid \mathbf{w}_1 - \mathbf{w}_2 \in \mathcal{C}\} \rangle \subseteq \mathbb{K}[x_1, \dots, x_n] \quad (1)$$

where the characteristic crossing function $\mathbf{a} : \mathbb{Z}_2^n \rightarrow \mathbb{Z}^n$ replaces the class of 0, 1 by the same symbols regarded as integers; \mathbb{K} is an arbitrary field and if $\mathbf{a}^{\mathbf{w}} = (w_1, \dots, w_n)$ then $\mathbf{x}^{\mathbf{a}^{\mathbf{w}}} = \prod x_i^{w_i}$. If we consider a degree compatible ordering \prec and we compute a Gröbner basis \mathcal{G}_{\prec} w.r.t. \prec of the ideal $\mathcal{I}_{\mathcal{C}}$ the normal form of any monomial $\prod x_i^{w_i}$ corresponds with the syndrome of the word $\nabla(w_1, \dots, w_n)$ where the map ∇ is reduction modulo 2. Thus we can take N in Definition 4 as the vectors $\nabla(w_1, \dots, w_n)$ such that $\prod x_i^{w_i}$ is a normal form w.r.t. \mathcal{G}_{\prec} , i.e. the syndromes of the code. Note also that ϕ is just given by the multiplication tables of the normal forms times the variables x_i in the ring $\mathbb{K}[x_1, \dots, x_n]/\mathcal{I}_{\mathcal{C}}$. This is standar way of representing the quotient by an ideal $\mathcal{I}_{\mathcal{C}}$ using the FGLM algorithm (see [17] chapter 29 for a complete

reference on Gröbner basis topics). Moreover, the Gröbner representation of a code can be computed with a modification of the FGLM algorithm [5], one implementation in GAP [11] of this algorithm can be found in [7].

The binomial ideal $\mathcal{I}_{\mathcal{C}}$ can be seen also as a kernel of a modular integer linear program problem stated as follows. Let $H \in \mathbb{Z}^{m \times n}$ be a $m \times n$ matrix such that ∇H is a parity check matrix of \mathcal{C} and $\mathbf{b} \in \mathbb{Z}^m$.

$$IP_H(\mathbf{b}) \equiv \begin{cases} \min \{(1, 1, \dots, 1) \cdot \mathbf{u}^t\} \\ \mathbf{u} \in \mathbb{Z}_{\geq 0} \\ H \cdot \mathbf{u}^t = \mathbf{b} \bmod 2. \end{cases} \quad (2)$$

Ikegami and Kaji [12] studied the kernel of this problem related with the maximum likelihood decoding problem. It has been also studied in [16] in order to describe the combinatorics of the minimal codewords of the code \mathcal{C} .

Associated to the Gröbner representation we can define the *border of a code* [9] as follows

Definition 5. Let \mathcal{C} be a code and H a parity check matrix of \mathcal{C} , let (N, ϕ) be a Gröbner representation of $\mathbb{F}_2^n/\mathcal{C}$. Then the *border of the code* \mathcal{C} w.r.t. (N, ϕ) is the set

$$B(\mathcal{C}) = \{(\mathbf{n}_1 + \mathbf{e}_i, \mathbf{n}_2) \mid i \in \{1, \dots, n\}, \mathbf{n}_1 + \mathbf{e}_i \neq \mathbf{n}_2, \mathbf{n}_1, \mathbf{n}_2 \in N \text{ and } H \cdot (\mathbf{n}_1 + \mathbf{e}_i) = H \cdot \mathbf{n}_2\}, \quad (3)$$

An important remark is that both components of an element in the set $B(\mathcal{C})$ are in the same coset, i.e. their sum is in the code. We can also describe the border in as

$$B(\mathcal{C}) = \{(\mathbf{n} + \mathbf{e}_i, \phi(\mathbf{n}, \mathbf{e}_i)) \mid i \in \{1, \dots, n\}, \mathbf{n} \in N\} \setminus \{(\mathbf{x}, \mathbf{x})\}. \quad (4)$$

The border of a code $B(\mathcal{C})$ is associate to the border basis of the ideal $\mathcal{I}_{\mathcal{C}}$. The conection between the ideal \mathcal{G}_{\prec} comes from the well known fact that that every Gröbner basis with respect to a degree-compatible term ordering can be extended to a border basis (see [14, p. 281ff]) but not every border basis is an extension of a Gröbner basis. The preference of border bases over Gröbner bases in our case arises from the iterative generation of linear syzygies, inherent in the linear algebra algorithm used in [8], which allows for successively approximating the basis degree-by-degree, i.e. weight-by-weight.

IV. GRADIENT DESCENT DECODING AND REDUCTION

Given a code \mathcal{C} and its corresponding Gröbner representation (N, ϕ) we can accomplish two types of reduction that we will see are associated to Algorithms 1, 3 above. Thus both algorithms obey to the same algebraic structure.

A. Reduction by ϕ

We shall define the reduction of an element $\mathbf{n} \in N$ w.r.t. \mathbf{e}_i as the element $\mathbf{n}' = \phi(\mathbf{n}, \mathbf{e}_i)$ and we will denote it by $\mathbf{n} \rightarrow_i \mathbf{n}'$. For each $\mathbf{y} \in \mathbb{F}_2^n$, $\mathbf{y} = \mathbf{0} + \sum_j \mathbf{e}_{i_j}$ for some $i_j \in \{1, \dots, n\}$, thus we can iterate a finite number of reductions to find the representative of the coset $\bar{\mathbf{y}}$ containing \mathbf{y} . Note that in the case that we use \prec defined above the representatives of the classes corresponds with coset leaders, we will consider that this is

the case from now on. This gives us the following gradient descent decoding algorithm.

Algorithm 6. (N, ϕ) -reduction GDDA

Input: \mathbf{r} the received word.

Output: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to \mathbf{r}

Forward step

$\mathbf{r} = \sum_{j=1}^s \mathbf{e}_{i_j}$. Compute $\mathbf{n} \in N$ corresponding to the coset $\bar{\mathbf{r}}$, i.e.

a) $\mathbf{n} = \mathbf{0}$.

b) For $j = 1, \dots, s$ do

$$\mathbf{n} \rightarrow_{i_j} \mathbf{n}', \quad \mathbf{n} \leftarrow \mathbf{n}'$$

Backward step

While $\mathbf{n} \neq \mathbf{0}$

a) Compute \mathbf{r}' such that $\mathbf{r}' = \mathbf{r} + \mathbf{e}_{i_j}$ and

$$\text{wt}(\mathbf{n}) \geq \text{wt}(\phi(\mathbf{n}, \mathbf{e}_{i_j}))$$

b) $\mathbf{r} \leftarrow \mathbf{r}'$, $\mathbf{n} \leftarrow \phi(\mathbf{n}, \mathbf{e}_{i_j})$.

Return: $\mathbf{c} = \mathbf{r}$.

Note that the previous algorithm is somehow redundant, since at the end of the forward step we end with the coset leader \mathbf{n} of the class $\bar{\mathbf{r}}$, thus we can decode without performing the forward step. Anyway we have stated this way to see the resemblance with Algorithm 1. We can modify our algorithm capturing the needed information of the Gröbner representation as follows.

Definition 7. Let (N, ϕ) Gröbner representation of $\mathbb{F}_2^n / \mathcal{C}$ and $\{\mathbf{n}_i\}_{i=1}^{2^{n-k}}$ an ordering on N with $\mathbf{n}_1 = \mathbf{0}$. We will denote by (N^*, ϕ^*) the following pair.

$$N^* = \{(i, w_i) \in \mathbb{Z}_{\geq 0}^2 \mid w_i = \text{wt}(\mathbf{n}_i), i = 1, \dots, 2^{n-k}\}$$

$$\phi^* : N^* \times \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_n\} \rightarrow N^* \\ (i, w_i) \quad \phi^*((i, w_i), \mathbf{e}_j)$$

such that $\phi^*((i, w_i), \mathbf{e}_j) = (i_j, w_{i_j})$ if $\mathbf{n}_{i_j} = \phi(\mathbf{n}_i, \mathbf{e}_j)$ and $w_{i_j} = \text{wt}(\mathbf{n}_{i_j})$.

In other words, we keep track only on the ordering of the normal forms representing each coset and the weight of one of its leaders. Note that (N^*, ϕ^*) can be easily computed from a Gröbner representation (N, ϕ) w.r.t. a degree compatible ordering \prec since for \prec the normal forms are coset leaders. Moreover, the way of computing a Gröbner representation by FGLM techniques gives us an incremental construction of N^* ordered non-decreasingly on the second component (see [4] for further details), i.e.

$$(i, w_i), (j, w_j) \in N^* \text{ and } i < j \Rightarrow w_i \leq w_j.$$

Now it is clear that we can decode using only (N^*, ϕ^*) , thus we can avoid storing the normal forms in the Gröbner representation.

Algorithm 8. (N^*, ϕ^*) -reduction GDDA

Input: \mathbf{r} the received word.

Output: A codeword $\mathbf{c} \in \mathcal{C}$ that is closest to \mathbf{r}

Forward step

$\mathbf{r} = \sum_{j=1}^s \mathbf{e}_{i_j}$. Compute $\ell \in \{1, \dots, 2^{n-k}\}$ corresponding to the coset $\bar{\mathbf{r}}$, i.e.

a) $i = 1, w_1 = 0$.

b) For $j = 1, \dots, s$ do

$$\phi^*((i, w_i), \mathbf{e}_{i_j}) = (i', w'_i), \quad (i, w_i) \leftarrow (i', w'_i)$$

Return $i = \ell$.

Backward step

While $i \neq 1$

a) Compute \mathbf{r}' such that $\mathbf{r}' = \mathbf{r} + \mathbf{e}_{i_j}$ and

$$w_i \geq w'_i$$

where w'_i is the second component of $\phi^*((i, w_i), \mathbf{e}_{i_j})$

b) $\mathbf{r} \leftarrow \mathbf{r}'$, $(i, w_i) \leftarrow \phi^*((i, w_i), \mathbf{e}_{i_j})$.

Return: $\mathbf{c} = \mathbf{r}$.

As an intermediate result, from the forward step we already know if the coset has a correctable leader if $w_\ell \leq t = \lfloor \frac{(d-1)}{2} \rfloor$, in that case the backward step gives us a unique solution, if $\ell > t$ then there could be multiple ways of doing the backtracking step depending on the number of leaders in the ℓ -th-coset. Also this algorithm can be used to answer the t -CWP problem.

Note that the backward step is just the l-GDDA in Algorithm 1. As pointed by Liebler [15] in each step of the backtracking procedure we change of coset till we arrive to the $\bar{\mathbf{0}}$ coset.

B. Border reduction

Now taking into account the information on the border of the code $B(\mathcal{C})$, we can make a similar reduction substituting in each step the first component of an element of the border by the second one. More formally, let $(\mathbf{b}_1, \mathbf{b}_2) = \mathbf{b} \in B(\mathcal{C})$, we define the *head* and the *tail* of \mathbf{b} as

$$\text{head}(\mathbf{b}) = \mathbf{b}_1, \text{tail}(\mathbf{b}) = \mathbf{b}_2 \in \mathbb{F}_2^n.$$

As pointed before $\text{head}(\mathbf{b}) + \text{tail}(\mathbf{b})$ is a codeword of \mathcal{C} for all $\mathbf{b} \in B(\mathcal{C})$ and by its definition (3) it is clear that the information in the border allows complete decoding. The information in the border is somehow redundant, we can reduce the number of codeword in it needed for decoding.

Definition 9. A set $R(\mathcal{C})$ is the *reduced border* for the code \mathcal{C} with respect to the order \prec if $R(\mathcal{C}) \subseteq B(\mathcal{C})$ and it fulfills the following conditions:

1) For each pair $(\mathbf{n}, \mathbf{e}_i)$ such that $\mathbf{n} + \mathbf{e}_i$ is a head in $B(\mathcal{C})$ there exists an element in $R(\mathcal{C})$ such that its head is \mathbf{h} where

$$\text{supp}(\mathbf{h}) \subseteq \text{supp}(\mathbf{n} + \mathbf{e}_i).$$

2) Given two elements in $R(\mathcal{C})$ and $\mathbf{h}_1, \mathbf{h}_2$ their heads, then we have that

$$\text{supp}(\mathbf{h}_1) \not\subseteq \text{supp}(\mathbf{h}_2) \text{ and } \text{supp}(\mathbf{h}_2) \not\subseteq \text{supp}(\mathbf{h}_1).$$

Thus $R(\mathcal{C})$ is the set with smallest cardinal that allows us a gradient-like test set decoding using reductions.

Proposition 10. *Let us consider the set of codewords in \mathcal{C} given by*

$$\text{Min}_{red}(\mathcal{C}) = \{\text{head}(\mathbf{b}) + \text{tail}(\mathbf{b}) \mid \mathbf{b} \in R(\mathcal{C})\} \subseteq \mathcal{C}. \quad (5)$$

Then $\text{Min}_{red}(\mathcal{C}) \subseteq \mathcal{M}_{\mathcal{C}}$.

Proof: Let $\text{head}(\mathbf{b}) + \text{tail}(\mathbf{b}) = \mathbf{c}$ where $\mathbf{b} \in R(\mathcal{C})$ and suppose $\mathbf{c} \notin \mathcal{M}_{\mathcal{C}}$, then there exists $\mathbf{c}' \in \mathcal{C}$ such that $\text{supp}(\mathbf{c}') \subset \text{supp}(\mathbf{c})$. Let \mathbf{c}_1 be a vector such that $\text{supp}(\mathbf{c}_1) = \text{supp}(\mathbf{c}) \cap \text{supp}(\text{head}(\mathbf{b}))$, thus $\mathbf{c}_2 = \mathbf{c} - \mathbf{c}_1$ fulfills $\text{supp}(\mathbf{c}_2) \subset \text{supp}(\text{tail}(\mathbf{b}))$. Let \mathbf{m} be the maximum between \mathbf{c}_1 and \mathbf{c}_2 , therefore $\text{supp}(\mathbf{m}) \subset \text{supp}(\mathbf{c})$, and \mathbf{m} is smaller than $\text{head}(\mathbf{b})$ and $\text{tail}(\mathbf{b})$ which contradicts the fact that $R(\mathcal{C})$ is reduced. ■

Therefore the set $\text{Min}_{red}(\mathcal{C})$ is a minimal test set w.r.t. the order \prec given by minimal codewords that allow the ts-GDD algorithm stated in Algorithm 3. It can be also seen as a test set for the modular integer program in Equation (2).

CONCLUSIONS

We have shown an unified approach via the Gröbner presentation of a code to two gradient descent decoding algorithms, one that the search is done changing the coset representative (l-GDDA) and the one given by descending within the same coset (ts-GDDA) that were claimed to be of different nature. This two algorithms come from two ways of computing the reduction of a monomial modulo a binomial ideal associated to the code. Unfortunately there are some obstructions for generalizing this approach in a straightforward way to non binary codes mainly motivated by the non-admissibility of the ordering needed for decoding (see [4]). Further research lines of the authors point to generalizing the border basis for the non binary case in order to describe the set of minimal codewords of a code.

REFERENCES

- [1] A. Ashikhmin and A. Barg, *Minimal vectors in linear codes* IEEE Trans. Inform. Theory **44** (1998), 2010–2017.
- [2] A. Barg, *Complexity issues in coding theory*, In Handbook of Coding Theory, Elsevier Science, Vol. 1, (1998), 649–754
- [3] E.R. Berlekamp, R.J. McEliece, H.C.A. van Tilborg, *On the Inherent Intractability of Certain Coding Problems* IEEE Trans. Inform. Theory, **IT-24**, no. 3, (1978), 384–386.
- [4] M. Borges-Quintana, M.A. Borges-Trenard and E. Martínez-Moro, *On a Gröbner bases structure associated to linear codes*, J. Discrete Math. Sci. Cryptogr. **10** (2007), no. 2, 151–191.
- [5] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *A general framework for applying FGLM techniques to linear codes*, AAECC 16, Lecture Notes in Comput. Sci., **3857**, (2006), 76–86.
- [6] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *A Gröbner representation of linear codes*, In: T. Shaska, W.C. Huffman, D. Joyner, V. Ustimenko (eds.) Advances in Coding Theory and Cryptography, World Scientific (2007), 17–32.
- [7] M. Borges-Quintana, M.A. Borges-Trenard, E. Martínez-Moro, *GBLA-LC: Gröbner Bases by Linear Algebra and Linear Codes*, In: ICM 2006. Mathematical Software, EMS, (2006), 604–605.
- [8] M. Borges-Quintana, M.A. Borges-Trenard, P. Fitzpatrick, E. Martínez-Moro, *On a Gröbner bases and combinatorics for binary codes*, Appl. Algebra Engrg. Comm. Comput. **19** (2008) 393–411.
- [9] M. Borges-Quintana, M.A. Borges-Trenard, I. Márquez-Corbellá, E. Martínez-Moro, *On the Border of a Binary Code*. Submitted to Jour. Comp. Applied Maths.(2009).
- [10] J. Bruck, M. Naor, *The Hardness of Decoding Linear Codes with Preprocessing*, IEEE Trans. Inform. Theory **36**, no. 2, (1990)
- [11] The GAP Group, GAP – Groups, Algorithms, and Programming. Version 4.12 (2009). <http://www.gap-system.org>.
- [12] D. Ikegami and Y. Kaji, *Maximum likelihood decoding for linear block codes using Gröbner bases*, IEICE Trans. Fund. Electron. Commun. Comput. Sci. E86-A , **3** (2003) 643–651.
- [13] A. Kehrein and M. Kreuzer, *Characterizations of border bases*.Journal of Pure and Applied Algebra, **196** (2005), 251–270.
- [14] A. Kehrein and M. Kreuzer, *Computing border bases*. Journal of Pure and Applied Algebra, **205**, (2006) 279–295.
- [15] R. Liebler, *Implementing gradient descent decoding*, Michigan Math. J. **58** , Issue 1 (2009), 285–291.
- [16] I. Márquez-Corbellá, E. Martínez Moro, *Combinatorics of minimal codewords of some linear codes*, Submitted to Advances in Mathematics of Communications (2010).
- [17] T. Mora, *Solving polynomial equation systems. II. Macaulay's paradigm and Gröbner technology*, Encyclopedia of Mathematics and its Applications, 99. Cambridge University Press, Cambridge, (2005).